SYSTEM AND METHOD FOR DOWNLOADING APPLICATION COMPONENTS TO A CHIPCARD

Abstract of the Disclosure

The present invention describes a method for downloading application components, so-called on-card application components, from a server via a client to a chipcard, wherein the server and the client communicate with each other via a distributed system, in particular an Intranet or the Internet. The advantages of the present invention lie in the fact that downloading of the application components is divided into two stages: The first stage occurs on the server only, and ensures that not every command to download the application component is sent individually over the network. This is effected by means of a broadband-optimized protocol which bundles the individual commands to download the application component into a command sequence and sends it as a complete data packet over the network. This reduces the time required for downloading application components over the network. Each command within the command sequence is assigned a digital signature and, where appropriate, encrypted. This ensures that only authenticated commands are accepted by the chipcard. In this way this invention meets security requirements for the transfer of data via distributed systems, in particular over the Internet. The second stage occurs between the client and the chipcard, and ensures that the data packets are unpacked and sent individually to the chipcard. All security-relevant keys and certificates are stored on the

secure server. Communication between the client and the server runs preferentially via SSL (Secure Sockets Layer) as the transfer protocol. Misuse of the inventive system/method is thereby rendered much more difficult.